REMARKS

Applicants respectfully request further examination and reconsideration in view of the instant response. Claims 1-20 are pending in the application. Claims 1-20 are rejected.

REJECTIONS

35 U.S.C. §102(e) – Claims 1-20

The Office Action mailed February 14, 2008, states that Claims 1-20 are rejected under 35 U.S.C. §102(e) as being anticipated by Shanklin et al. (US Pat. 6,568,147), hereinafter called "Shanklin." Applicants have reviewed Shanklin, and respectfully submit that the embodiments of the present invention as recited in Claims 1-20 are not anticipated by Shanklin in view of at least the following rationale.

MPEP §2131 provides:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). … "The identical invention must be shown in as complete detail as is contained in the ... claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

Applicants respectfully submit that the rejection of the claims is improper as the rejection of Claims 1-20 does not satisfy the requirements of a *prima facie* case of anticipation as claim embodiments are not met by Shanklin. Applicants

respectfully submit that Shanklin does not teach or suggest the claimed embodiments in the manner set forth in independent Claims 1, 8 and 15.

Independent Claim 1 recites (emphasis added):

> 1. A method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:
> providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;
> receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and
> automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

Independent Claim 8 and 15 recite similar embodiments to Claim 1. Moreover, Claims 2-7 that depend from independent Claim 1, Claims 9-14 that depend from independent Claim 8 and Claims 16-20 that depend from independent Claim 15 also include these embodiments. Applicants respectfully submit that Shanklin does not teach, describe or suggest "providing … so that utilization of each network intrusion detection system can be based on demand … in said dynamic data center; receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and automatically arranging the monitoring of said monitoring

points using said network intrusion detection systems and said monitoring policy" as claimed.

The Office Action mailed February 14, 2008, states in part (section 2, paragraph 4, pg. 3, ff.) (emphasis added):

> "Regarding claims 1, 8 and 15, Shanklin et al., (emphasis in original) discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for managing utilization of network intrusion detection systems in a dynamic data center, said method comprising: providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center (column 2 lines 48-50 — "Multiple intrusion detection sensors are used at the entry point to the network, specifically, at an 'internetworking device' such as a router or a switch" and column 2 lines 54-56 — "internetworking device, whether a router or switch, is processor-based and includes load balancing programming, which controls how packets are distributed from the internetworking device to the sensors for processing"); receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems (column 2 lines 1-13 — Shanklin et al. (emphasis in original) discloses the claimed "monitoring policy" as being inclusive to the IDS sensors, which comprise: "packet load to the sensors that is 'load balanced', such that said packets are distributed at least at a session-based level [or] packet-based level ... the results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain unauthorized access to the network"); and automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy ("column 5 lines 19-20 — Shanklin et al. (emphasis in original) again discloses the "monitoring points" as being inclusive to the IDS sensors, which comprise "load balancing unit, which distributes packet among the sensors," which can be "session-based (column 5 line 22)" or "network-based (column 5 line 58)").

Shanklin et al. (emphasis in original) recites a local network "having a mesh topology … [and] interconnected computer stations l0a, typically having a server l0b to function as a sort of gateway to network resources," which is equated to the dynamic data center mentioned in the preamble.

Shanklin et al. (emphasis in original) recites intrusion detection sensors which "autonomously comprise the entire intrusion detection system (column 3 lines 58-62).

Therefore, the Examiner understands the disclosed "multiple intrusion detection sensors" to comprise the function of claimed plurality of network intrusion detection system, monitoring points and monitoring policy. Thus the disclosure of Shanklin et al. (emphasis in original) highlights the various elements and components of the disclosed "multiple intrusion detection sensors are used at the entry point to the network, specifically, at an 'Internetworking device' such as a router or a switch."

The Office Action asserts that Shanklin teaches the embodiment "dynamic data center" in the claim language of Claim 1 as "a local network 'having a mesh topology …" found in Shanklin at column 3, lines 49-53:

> "Although local network 10 is illustrated as having a "mesh" type topology, this is for purposes of example. Local network 10 could be any system of interconnected computer stations 10a, typically having a server 10b to function as a sort of gateway to network resources." (Emphasis added.)

But, referring to Shanklin's title and abstract, among other places, Applicants understand Shanklin to teach parallel intrusion detection sensors with load balancing for high speed networks where multiple sensors are connected at an internetworking device, which can be a router or a switch. Shanklin does not mention a "dynamic data center" and therefore Applicants do not understand Shanklin to teach "said network intrusion detection systems in said dynamic data

center," as recited by Claim 1. As Applicants understand Shanklin "a local network 'having a mesh topology ..." is defined by Shanklin at column 3, lines 51-53 as "any system of interconnected computer stations 10a, typically having a server 10b to function as a sort of gateway to network resources." Applicants do not understand a "dynamic data center" to be "a local network," as Shanklin has defined above. Therefore, Applicants respectfully disagree with the Office Action's "equating" the term "dynamic data center" to "a local network."

Moreover, Applicants note that the Office Action mailed February 14, 2008, states "the dynamic data center mentioned in the preamble" (section 2, paragraph 5, pg. 3). As terms mentioned in the preamble are sometimes not given the same patentable weight of embodiments in the body of the claim, Applicants respectfully note that the embodiment, "dynamic data center," is also to be found in the body of Claim 1, not solely in the preamble to Claim 1, and as such should be given its full patentable weight in construing Claim 1. (Emphasis added.)

Applicants respectfully submit that Shanklin does not disclose nor teach "providing ... so that utilization of each network intrusion detection system can be based on demand ... in said dynamic data center," as claimed. Therefore, Applicants submit that Shanklin fails to disclose each and every element of Claim 1, arranged as required by the Claim. As similar embodiments are found in independent Claims 8 and 15, Applicants respectfully assert that Shanklin does

not teach, disclose or suggest the claimed embodiments as recited in independent Claims 1, 8 and 15. As the claimed embodiments are not met by Shanklin, Applicants respectfully submit that the rejection does not satisfy the requirements of a *prima facie* case of anticipation. Therefore, Applicants respectfully submit that Claims 1, 8 and 15 overcome the rejection under 35 U.S.C. § 102(e), and that these claims are thus in a condition for allowance.

Similarly, Applicants respectfully submit that Shanklin also does not teach or suggest the claimed feature, "providing … so that utilization of each network intrusion detection system can be based on demand … in said dynamic data center," as recited in Claims 2-7 that depend from independent Claim 1, Claims 9-14 that depend from independent Claim 8 and Claims 16-20 that depend from independent Claim 15. Therefore, Applicants respectfully submit that Claims 2-7, Claims 9-14 and Claims 16-20 also overcome the rejection under 35 U.S.C. § 102(e), and are in a condition for allowance as being dependent on allowable base claims.

CONCLUSION

Based on the arguments presented above, Applicants respectfully assert that Claims 1-20 overcome the rejections of record and, therefore, Applicants respectfully solicit allowance of these claims.

The Examiner is invited to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Respectfully submitted,

WAGNER BLECHER L.L.P.

Dated: 05/13/2008

/John P. Wagner, Jr./
John P. Wagner, Jr.
Registration No. 35,398

123 Westridge Dr.
Watsonville, CA 95076
(408) 377-0500